UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/756,904	01/14/2004	Marc A. Boulanger	RPS920030037US1	3081

45211 7590 04/09/2008

Robert A. Voigt, Jr.
WINSTEAD SECHREST & MINICK PC
PO BOX 50784
DALLAS, TX 75201

EXAMINER	
SCHMIDT, KARL	

ART UNIT	PAPER NUMBER
2139	

MAIL DATE	DELIVERY MODE
04/09/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/756,904	BOULANGER ET AL.	
	Examiner	Art Unit	
	KARI L. SCHMIDT	2139	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *30 January 2008*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-5* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-5* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *14 January 2007* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Notice to Applicant

This communication is in response to the amendment filed on 01/30/2008. Claims 1-5 remain pending. Claims 6-21 have been canceled.

Response to Arguments

Applicant's arguments, filed 01/30/2008, with respect to the rejections of claims 1-5 under 35 U.S.C 102 (e) have been fully considered and are persuasive. Therefore, the rejection has been withdrawn. However, upon further consideration, a new ground(s) of rejection is made in view of Hershey, Lingafelt and Kodashiro.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1-3 and 5 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hershey et al. (US 5,414,833) in view of Lingafelt et al. (US 2004/0199790 A1).

Claim 1

Hershey discloses a method for rapid intrusion detection for network communication (see at least, col. 6, lines 65-67 and col. 7, lines 22-40: the examiner notes the method which provides a security agent, constant monitoring means and responding means

which responds to a detected security event in a high-speed data communications network) and coupling selected data from the network data to a parallel pattern detection engine (PPDE), for comparing the selected data in parallel to M sequences of pattern data stored in the PPDE and generating a match output signal when at least one of the M sequences of pattern data compares to a portion of the selected data (see at least, col. 13, lines 26-48 and col. 13, line 66 - col. 14, line 12: the examiner notes the use of a parallel finite state machine adaptive monitor as an IC which performs parallel pattern detection of an incoming bit stream and further the parallel finite state machine is connected to a plurality of FSMs which perform a respective analysis of a bit stream (col. 13, lines 62-65). Further the examiner notes that each FSM is tied in with an start and terminate signal for the progression of the FSMs analysis of the bit stream (col. 14, lines 13-31 and col. 14, lines 40-67). Further the examiner notes the FSMs contain a M sequence of pattern data stored within the FSMs to the incoming bit stream for pattern detection (col. 15, line 59 - col. 16, line 40)).

Hershey fails to specifically disclose receiving packets of network data in a network processor coupled to a network fabric and forwarding routed network data to the network fabric.

However, Lingafelt discloses a method for rapid intrusion detection for network communication (see at least, abstract: the examiner notes a method for detecting attempted intrusions into a network and [0005]) and receiving packets of network data in a network processor coupled to a network fabric (see at least, FIG. 3 and [0016]: the examiner notes all packets are sent to the network processor); forwarding routed

network data to the network fabric (see at least, FIG. 3 and [0016]: the examiner notes all packets from the network processor are forwarded to the network fabric) and further the network fabric coupled to the network intrusion detection system (see at least, FIG. 3 and [0016]: the examiner notes all packets with patterns of interest are received for processing at a network intrusion detection system).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the teachings of Hershey's rapid intrusion detection to include receiving packets of network data in a network processor coupled to a network fabric and forwarding routed network data to the network fabric as taught by Lingafelt. One of ordinary skill in the art would have been motivated to combine the teachings in order to provide an improved method for detecting attempted intrusions into a network without compromising the performance of the intrusion detection system (see at least, Lingafelt, [0004]).

Claim 2

Hershey discloses further comprising the steps of storing N pattern data in the M PUs sequences of pattern data with corresponding identification (ID) data used to identify which of the N pattern is detected (see at least, col. 15, line 59 - col. 16, line 40: the examiner notes the FSMs detect a given sequences of pattern data based of the identification of the pattern data (e.g. "JOHN", "JIM", etc) which are stored within each FSM (e.g. M PUs)) and storing action code indicating action to take in response to detecting a particular one of the N pattern data (see at least, col. 15, line 59 - col. 16,

line 60: the examiner notes an alarm is triggered with response to identifying a given particular N pattern data (e.g. "JOHN", "JIM", etc) in which a action code with response to be performed (e.g. SA modifies, injects, or deletes) for the pattern from the bit stream).

Hershey fails to specifically disclose N pattern data is N intrusion signatures.

However, Lingafelt discloses wherein N pattern data can be intrusion signatures (see at least, [0002]: the examiner notes examination of packets for patterns of interest is also known as intrusion detection signatures).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the teachings of Hershey's rapid intrusion detection to include detecting N intrusion signatures (also known as patterns) as taught by Lingafelt . One of ordinary skill in the art would have been motivated to combine the teachings in order to provide an improved method for detecting attempted intrusions into a network without comprising the performance of the intrusion detection system (see at least, Lingafelt, [0004]).

Claim 3

Hershey discloses analyzing a bit stream of data and generating a particular pattern analysis (see at least, col. 13, lines 1-47 and col. 13, line 66 - col. 14, line 12: the examiner notes the analysis of characteristic pattern data within the parallel finite sate machine) and comparing the selected pattern data to the store of N pattern data and generating at network data speed, a pattern compare signal and particular ID data when

a particular one of the N intrusion signatures is detected (see at least, col. 15, line 59 - col. 16, line 60: the examiner notes the FSMs detect a given sequences of pattern data based of the identification of the pattern data (e.g. "JOHN", "JIM", etc) which are stored within each FSM (e.g. M PUs) and the examiner notes an alarm is triggered with response to identifying a given particular N pattern data (e.g. "JOHN", "JIM", etc) in which a action code with response to be performed (e.g. SA modifies, injects, or deletes) for the pattern from the bit stream. Further the examiner notes the following is performed in real time monitoring of the data patterns in their actual network traffic (see at least, col. 12, line 26-33).

Hershey fails to disclose the use of packets of network data and generating a valid packet of network data as the selected data to compare again an N intrusion signature.

However, Lingafelt discloses the use of packets of network data and generating a valid packet of network data as the selected data to compare again an N intrusion signature (see at least, [0002]: the examiner notes examination of packets for patterns of interest is also known as intrusion detection signatures and [0017]: the examiner notes the use of pattern matching of packets in memory with the plurality of packet segments from the transmission). Lingafelt discloses wherein N pattern data can be intrusion signatures (see at least, [0002]: the examiner notes examination of packets for patterns of interest is also known as intrusion detection signatures).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the teachings of Hershey's rapid intrusion detection to

include the use of packets of network data and generating a valid packet of network data as the selected data to compare again an N intrusion signature as taught by Lingafelt. One of ordinary skill in the art would have been motivated to combine the teachings in order to provide an improved method for detecting attempted intrusions into a network without comprising the performance of the intrusion detection system (see at least, Lingafelt, [0004]).

Claim 5

Hershey discloses wherein the PPDE further comprises cascade circuitry coupled from each of the M PUs to one or more adjacent PUs within the M PUs for selectively coupling chain data between one or more groups of two or more adjacent PUs selected from the M PUs in response to the control data (see at least, col. 13, lines 1-47: the examiner notes the use of starting signals to start different FSMs for parallel pattern detection and further the use of programmable cross point which is what controls the cascading of the plurality of adjacent PUs (col. 14, lines 14-31)).

Claim 4 is rejected under 35 U.S.C. 103(a) as being unpatentable over Hershey et al. (US 5,414,833) in view of Lingafelt et al. (US 2004/0199790 A1), as applied to claim 3 above, and in further view of Kodashiro (US 5,831,997).

Claim 4

Hershey discloses wherein the PPDE comprises an input/output (I/O) interface for coupling data into and out of the PPDE (see at least, col. col. 13, lines 26-48: the examiner notes an input to all the FSMs and col. 16, lines 17-60: the examiner notes an output from the FSM (e.g. output alarm)); M processing units (PUs), each of the M PUs having compare circuitry for comparing each of the sequence of input data to pattern data stored in each of the M PUs and generating a compare output (see at least, col. 16, lines 8-50: the examiner notes the matching of characters (e.g. "F", "J", etc) as the means of comparing the input data to the pattern data and further the FSM is a IC circuit that is designed to allow such a comparison (col. 14, line 66-col.14, line 12)); an input bus for coupling the sequence of input data to each of the M PUs in parallel (see at least, col. 13, lines 1-48: the examiner notes the use of starting signals to initiate each FSM to work in parallel (FIG. 1A-1)); an output bus coupled to the I/O interface for sending output data to the I/O interface (see at least, FIG 1A-2: the examiner notes the I/O bus for the pattern alarms); control circuitry coupled to the I/O interface and coupling control data on a control data bus and identification (ID) on an ID bus to each of the M processing units (see at least, FIG 1B-1: the examiner notes all the FSMs are controlled with start signals from a bus for the analysis of corresponding data patterns (col. 14, line 2-12)); ID selection circuitry for selecting a match ID from ID data identifying the M PUs in response to a pattern match signal and match mode data (see at least, FIG. 1A and 1B: the examiner notes the use of the FSMs for pattern matching and start and terminate signals), wherein the match ID and match data corresponding to the match ID are saved in a temporary register as the output data (see at least, col. 10, line 41-66

and col. 14, line 40-col. 15, line 42: the examiner notes the address register stores the identity of the pattern (e.g. identity of the first FSM in the array)).

Hershey in view of Lingafelt fails to disclose wherein an address pointer selecting the pattern data in each of the M PUs is modified in response to a logic state of the compare output and an operation code stored with the pattern data.

However, Kodashiro discloses the use of address pointers for given data in memory based on the output of a logic state (see at least, abstract and FIG. 3: the examiner notes the decoders act as logic devices which in turn modify the address pointer for a given address in memory).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the teachings of Hershey and Lingafelt's rapid intrusion detection to include the use of address pointers for given data in memory based on the output of a logic state as taught by Kodashiro. One of ordinary skill in the art would have been motivated to combine the teachings in order to provide a pattern generating method by which locations in memory can be generated in such a way that various patterns can be used in common (see at least, Kodashiro, col. 2, lines 18-24).

Conclusion

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. See PTO-892.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to KARI L. SCHMIDT whose telephone number is

(571)270-1385. The examiner can normally be reached on Monday - Friday: 7:30am - 5:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kristine Kincaid can be reached on 571-272-4063. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Christian LaForgia/
Primary Examiner, Art Unit 2139

/Kari L Schmidt/
Examiner, Art Unit 2139